SOC Fundamentals

Presented by *Salman Qureshi*

Security Operations Center

- A dedicated unit is established by the organizations to handle and manage their security operations, known as Security Operation Center (SOC)

- It is centralized unit that continuously monitors and analyzes ongoing activities on an organization's information systems such as networks, servers, endpoints, databases, applications, websites, etc.

Need of SOC

Organizations use various security measures such as intrusion detection/prevention system, firewall, email filtering, URL filtering, and antivirus to protect the organization's network from threats.

However, in recent times, these security measures proved insufficient to provide enough security as hackers are inventing new trends and techniques to penetrate the network by evading such security measures. So, the need for such security measures that can keep the security perimeter always updated regarding new and developing threats and vulnerabilities. This is possible through SOC.

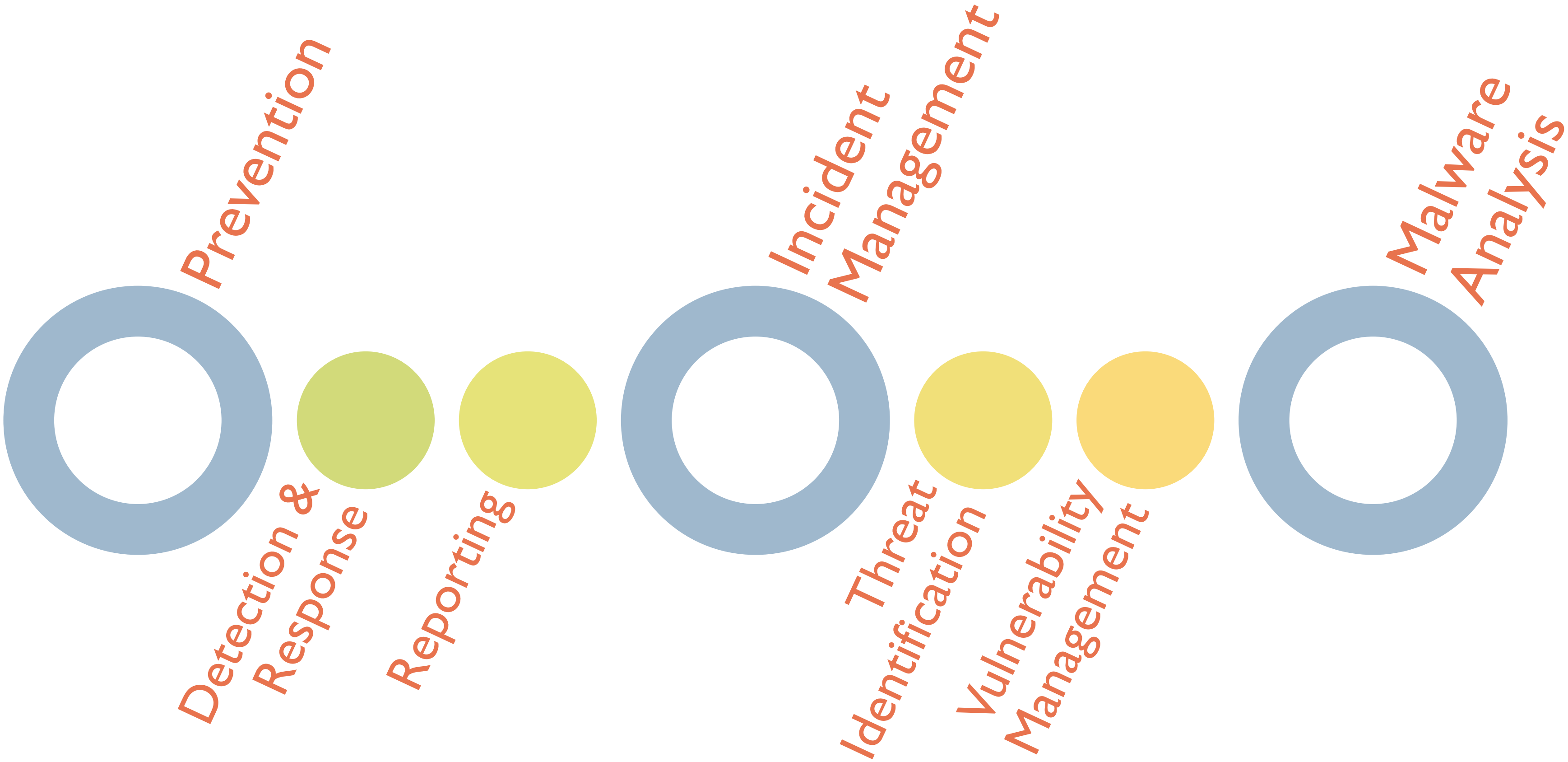
SOC is responsible for performing the following types of activities:

- Proactively identifying suspicious activities in the network and system.
- Performing vulnerability management to identify which activities are vulnerable to the network.
- Getting aware of hardware and software assets working in the network.
- Performing log management that facilitates forensics at the time of security breaches.
- Red, Blue and Purple teaming activities
- Threat Hunting
- Eradicating internal blinders.

SOC Essential Functions

- Network Security Monitoring
- Incident Response
- Forensics
- Command Center
- Threat Intelligence
- Self Assessment

SOC Capabilities



Prevention

Detection & Response

Reporting

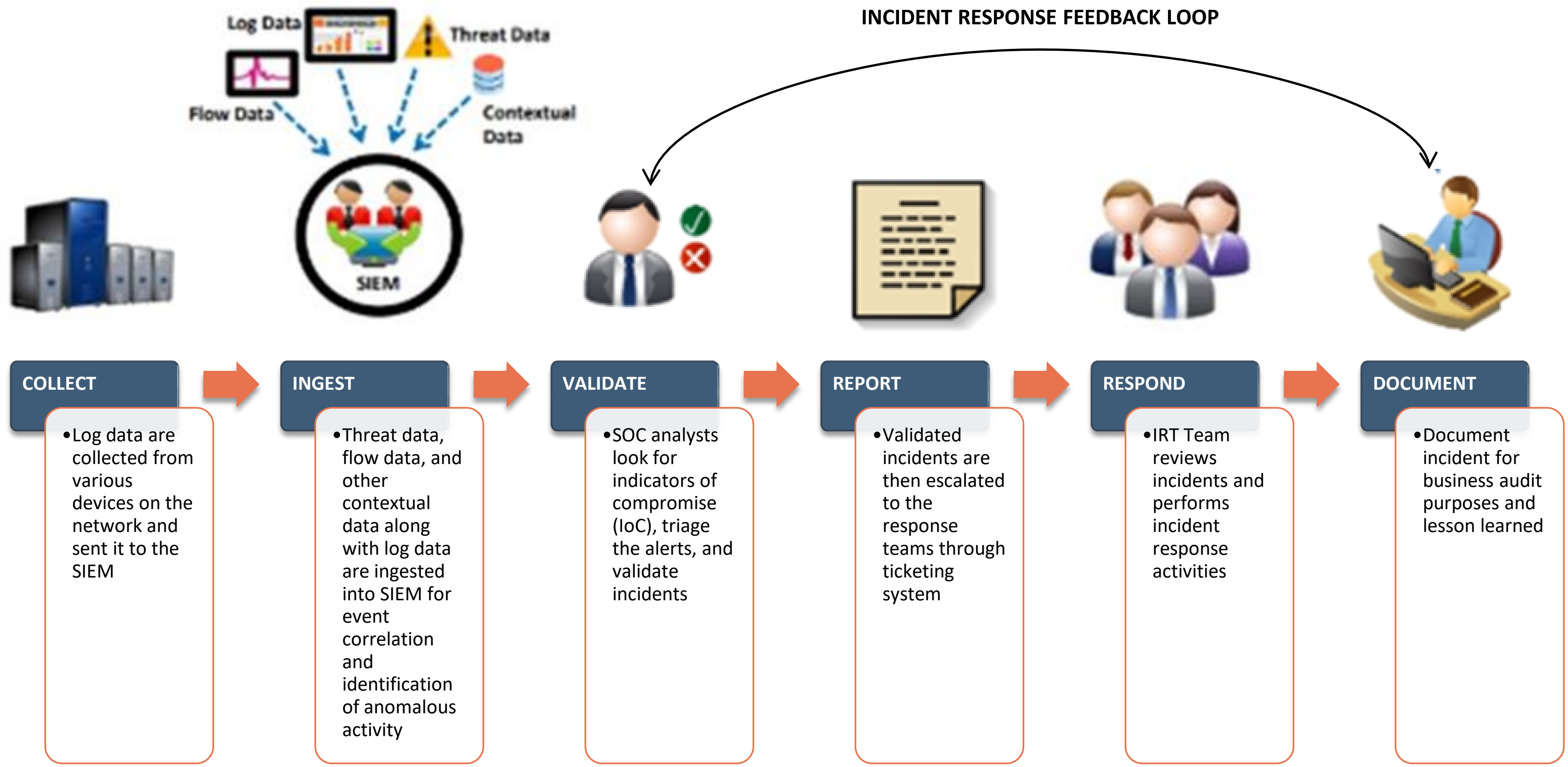
Incident Management

Threat Identification

Vulnerability Management

Malware Analysis

SOC Workflow



INCIDENT RESPONSE FEEDBACK LOOP

COLLECT

- Log data are collected from various devices on the network and sent it to the SIEM

INGEST

- Threat data, flow data, and other contextual data along with log data are ingested into SIEM for event correlation and identification of anomalous activity

VALIDATE

- SOC analysts look for indicators of compromise (IoC), triage the alerts, and validate incidents

REPORT

- Validated incidents are then escalated to the response teams through ticketing system

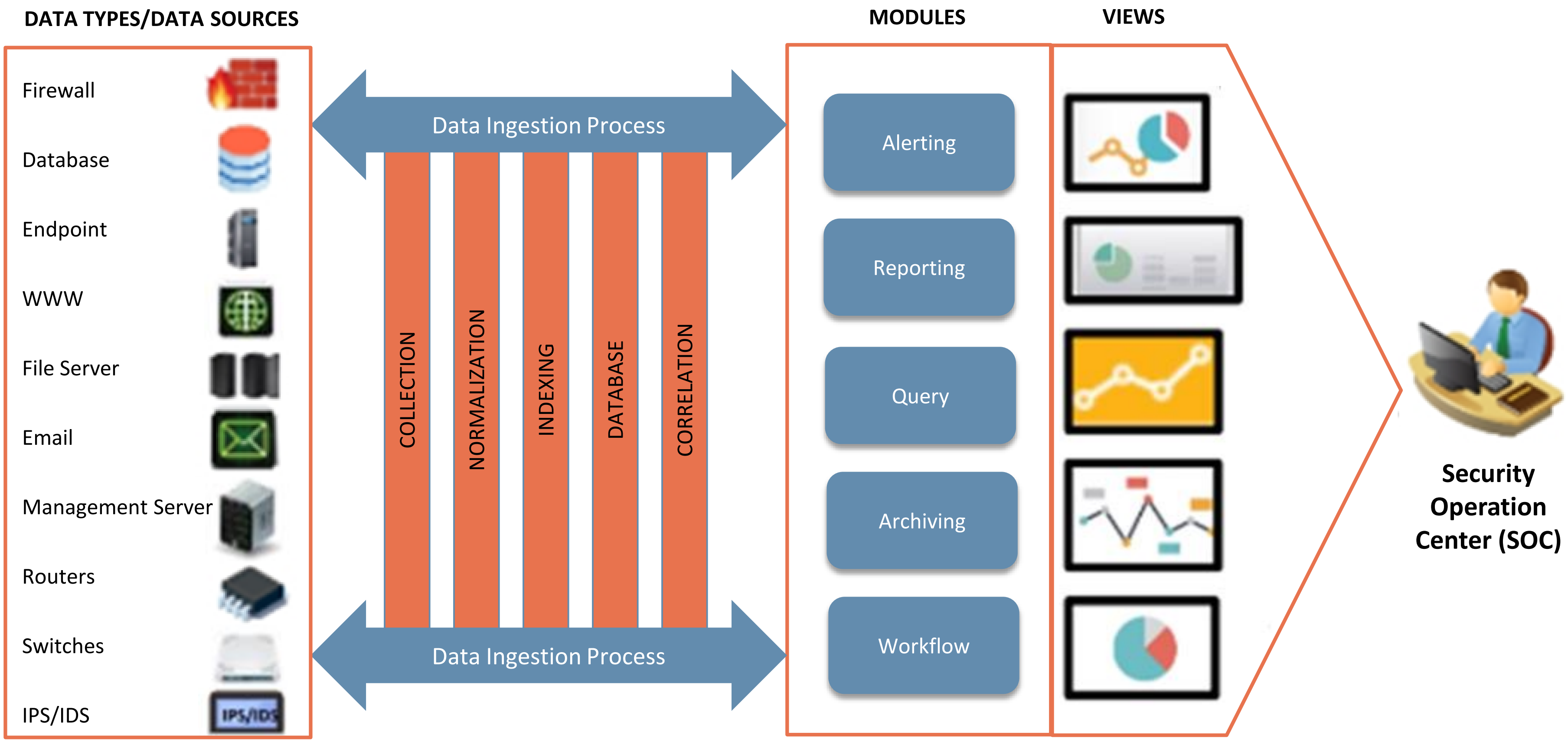
RESPOND

- IRT Team reviews incidents and performs incident response activities

DOCUMENT

- Document incident for business audit purposes and lesson learned

Security Dataflow



DATA TYPES/DATA SOURCES

- Firewall
- Database
- Endpoint
- WWW
- File Server
- Email
- Management Server
- Routers
- Switches
- IPS/IDS

Data Ingestion Process

COLLECTION

NORMALIZATION

INDEXING

DATABASE

CORRELATION

Data Ingestion Process

MODULES

- Alerting
- Reporting
- Query
- Archiving
- Workflow

VIEWS

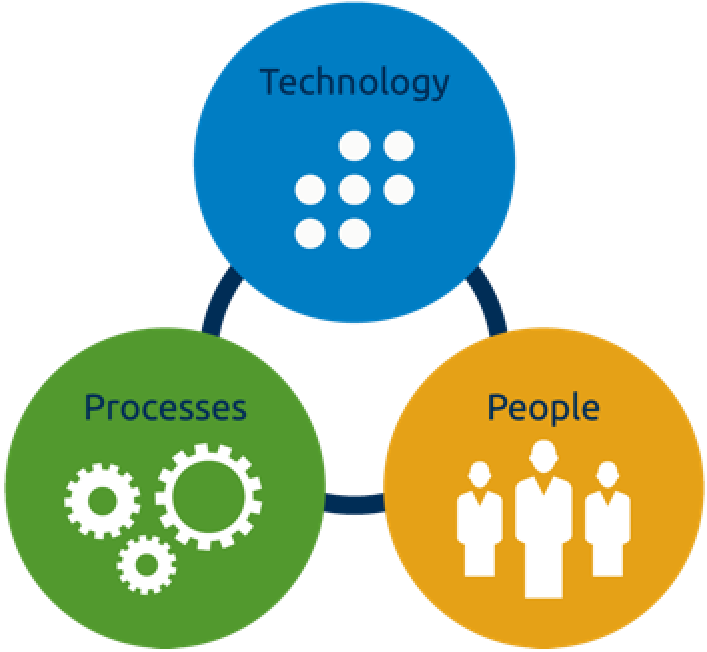
Security Operation Center (SOC)

Components of SOC: PP&T

A SOC requires cooperation and communication among People (Analyst, Operators, Administrators, Engineers, etc.) who monitor and analyze an organization’s IT infrastructure using the combination of Processes, Procedures, and Technology

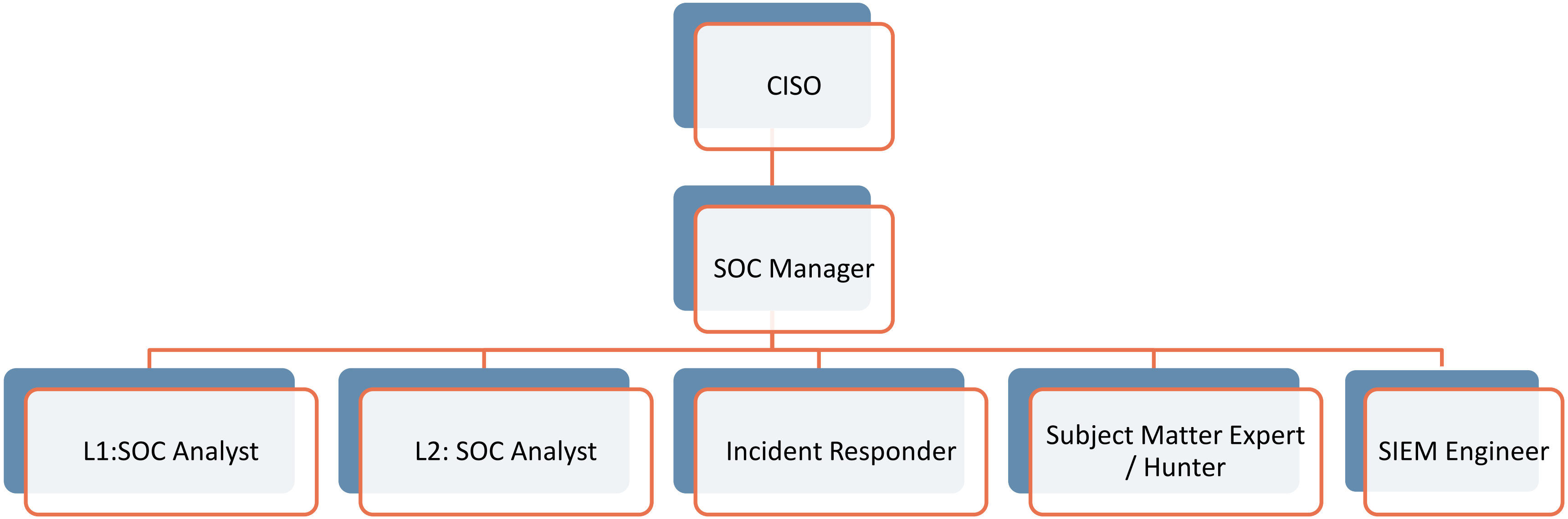
Skilled people for defined processes should have proper knowledge of intelligence technologies

Processes that are planned according to the technology should act as a connection between people and technology. They should ensure that both people and technology are operating adequately



Components of SOC: People

1. People are specialized individuals working at different levels of SOC
2. They should have deep technical knowledge, a wide range of capabilities, and a variety of experiences
3. They should be able to monitor and analyze a large amount of data/information that can be used for further investigations
4. They should possess the necessary training and certifications required to fulfill their respective roles and responsibilities



Components of SOC: Processes

- Processes are used by the different functional parts of the SOC to perform seamless and effective operations
- They behave as a link between people and technology
- The right team performs the right tasks through a well-defined process

01 Business Processes

- In the processes, administrative components are defined and documented for the efficient functioning of SOC
- They position the operations as per the organizational objectives
- Examples: report preparation, log retention, etc.

02 Technology Processes

- In these processes, actions related to IT infrastructure is defined and documented
- They ensure that IT infrastructure will works at best levels at any particular time
- Examples: Vulnerability scanning and remediation, firmware, etc.

03 Operational Processes

- These processes describe the different activities that are performed in a SOC
- Examples: Shift scheduling, Employee training

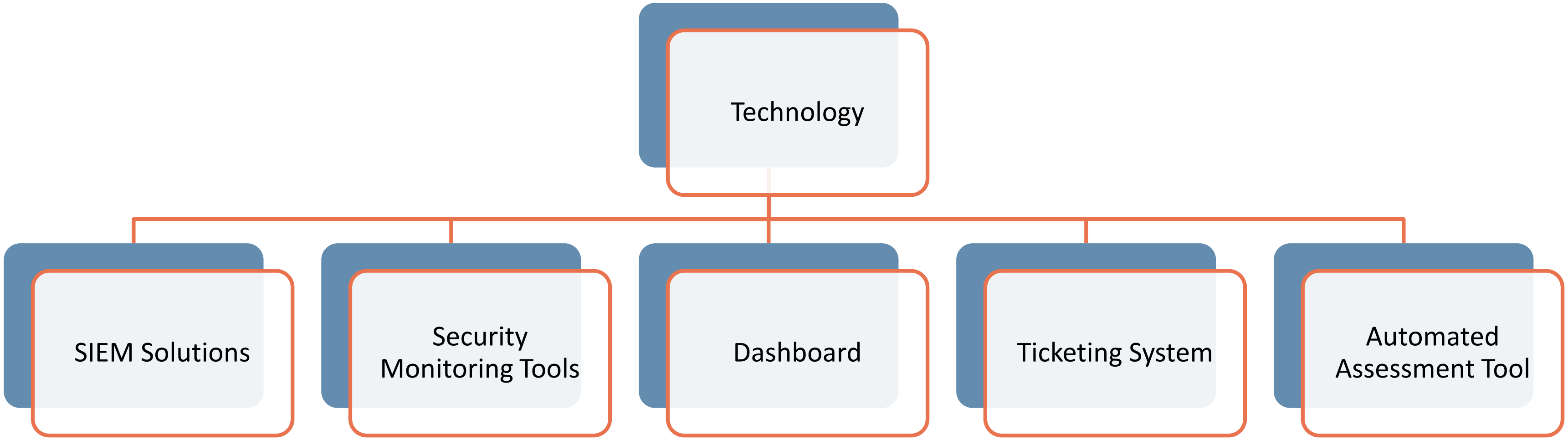
04 Analytical Processes

- Analytical processes explain the way to detect and remediate security issues
- They include different methods of identifying and understanding surfacing threats
- Examples: incident classification, detection and escalation, ticketing and forensics

Components of SOC: Technology

The organization should always select that technology that works for people and processes

The technology used in SOC should be collaborated efficiently to secure systems and networks



Types of SOC Models

The selection of a specific type of SOC model depends upon the requirements, processes, and day to day functionalities of an organization.

Three different types of SOC Models

1. In-House / Internal SOC Model
2. Outsourced SOC Model / SOC as a Service
3. Hybrid SOC Model

Types of SOC Models – In-House

- An in-house / internal SOC model is recommended to those organizations that have security issues related to outsourcing
- Outsourcing affects the integrity and functionality of the business

- Advantages:-
  - It helps the in-house staff to understand the organization and its environment in a much better manner, as compared to the third-party security service provider
  - It provides a complete picture related to the security posture of an organization

- Disadvantages:-
  - This model takes many years to set up infrastructure, threat intelligence, and other capabilities
  - It requires huge advance investment

Types of SOC Models - Outsourced

- It provides a robust security solution to the organization
- In this model, Managed Security Service Provider (MSSP) sets up the infrastructure and offers SOC monitoring and other capabilities
- It has a dedicated team of trained and experienced security analysts, who can monitor and analyze incidents, respond processes, aggregate technologies, correlate and analyze data, and perform threat research and intelligence on an ongoing basis

- Advantages:-
  - This model also helps the organization to meet specific compliance requirements
  - It offers cost-effective services as compared to in-house SOC model
  - It takes less time to build this model at an efficient level

- Disadvantages:-
  - It has the risk of external data mishandling
  - It does not provide long-term gain to the company

Types of SOC Models - Hybrid

- It is a combination of both in-house and outsourced SOC Model
- In this model, the organization is accompanied with MSSP to offer the most secure approach

- Advantages:-
  - They share synergies for technology, processes, expertise, facilitates, and personnel to reduce the cost
  - This model provides the best approach for monitoring and analyzing intrusion incidents, quick detection and response time, and low backlogs

- Disadvantages:-
  - It sets up extra hardware, managing data / information by the third party
  - It is expensive for long-term duration

SOC Maturity Models

Maturity models are IT governance tools that explain the organization’s working as per standardization, results, and measurement of effectiveness

They are used to analyze where a SOC succeeds and where it requires improvements

Few examples of maturity models include Control Objectives for Information Technology (CoBIT), Software Capability Maturity Model (CMMI), etc.

Types of Maturity Models:

01 SOC-Capability Maturity Model

02 Control Objectives for Information Technology (CoBIT)

03 National Institute of Standards and Technology (NIST) Cybersecurity framework

04 System Security Engineering Capability Maturity Model (SSE-CMM)

SOC Implementation

Planning

- Initial assessment is done based on existing capabilities with respect to people, processes, technology, business, and IT objectives
- SOC strategy development is carried out by considering its strategic goal, scope, model, services, KPI, metrics, etc.

Designing & Building the SOC

- Designing and building phases of SOC are almost linked to each other
- Selection of the best technology to implement efficient SOC is carried out in this phase

Operating the SOC

- SOC is moved from the building phase to the operating phase with the help of a proper transition plan

Reviewing & Reporting the SOC

- Review the SOC to identify the areas of improvement and to check whether it is operating accordingly

Challenges in SOC Implementation

1. Increasing the volume of security alerts
2. Management of numerous security tools
3. Lack of skilled analysts
4. Legal and regulatory compliance
5. Technology selection and configuration
6. Processes and procedures formalization, orchestration, and automation
7. Data integrity and intelligence management
8. Handling multi-staged advanced attacks
9. Rapid change in technology and security
10. Continuous training

SIEM Solutions

- Splunk
- IBM Qradar
- LogRhythm
- HP ArcSeight
- McAfee
- ClearSkies
- AlientVault
- SolarWinds

SOC Certifications

- Vendor Specific
  - Qradar
  - Splunk
  - LogRhythm
  - HP ArcSeight

- Non-vender (Neutral)
  - Cysa+
  - GCIH
  - GMON
  - EC Council CSA

Thanks !!!